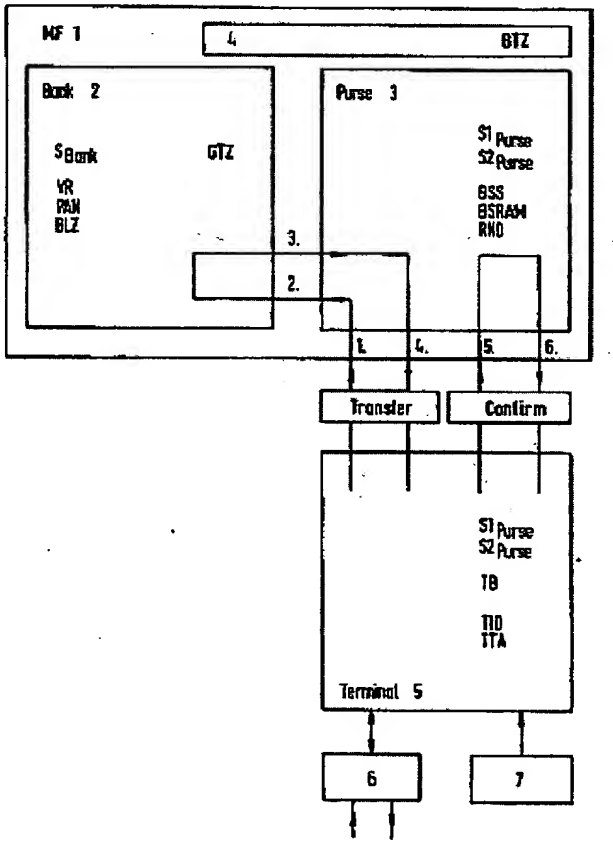
System for conducting transactions with a multifunctional card having an electronic purse

Patent number: DE4333388
Publication date: 1995-04-06
Inventor: RANKL WOLFGANG [DE]; WEIS DIETER [DE]
Applicant: GIESECKE & DEVRIENT GMBH [DE]
Classification:
- International: G07F19/00; G06K19/07; G06F17/60
- european: G07F7/08C; G07F7/08C2C
Application number: DE19934333388 19930930
Priority number(s): DE19934333388 19930930

Also published as:
EP0646898 (A2)
US5534683 (A1)
JP7254035 (A)
EP0646898 (A3)
EP0646898 (B1)

Abstract not available for DE4333388
Abstract of corresponding document: **US5534683**

In a system for conducting transactions with a multifunctional card having an integrated circuit, the circuit contains a bank application associated with the user's account-keeping bank and at least one purse application associated with a services supplier or manufacturer. With the aid of an apparatus communicating with the card, the card user can load a selectable sum of money into the purse application. The purse supplier is provided with a transaction certificate about the sum loaded in the purse and to be credited to the purse supplier's account, without a need for storing the secret data necessary for preparing this certificate in the purse application or in the purse terminal.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 43 33 388 A 1**

(51) Int. Cl.[6]:
G 07 F 19/00
G 06 K 19/07
G 06 F 17/60

(21) Aktenzeichen: P 43 33 388.5
(22) Anmeldetag: 30. 9. 93
(43) Offenlegungstag: 6. 4. 95

DE 43 33 388 A1

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(74) Vertreter:
Klunker, H., Dipl.-Ing. Dr.rer.nat.; Schmitt-Nilson, G., Dipl.-Ing. Dr.-Ing.; Hirsch, P., Dipl.-Ing., Pat.-Anwälte, 80797 München

(72) Erfinder:
Rankl, Wolfgang, 80797 München, DE; Weiß, Dieter, 88145 Hergatz, DE

(54) System zur Durchführung von Transaktionen mit einer Multifunktionskarte mit elektronischer Börse

(57) Bei einem System zur Durchführung von Transaktionen mit einer Multifunktionskarte mit integriertem Schaltkreis enthält der Schaltkreis eine der kontoführenden Bank des Benutzers zugeordnete Bankanwendung und wenigstens eine einem Dienstleistungsanbieter oder Hersteller zugeordnete Börsenanwendung. Mit Hilfe einer mit der Karte kommunizierenden Vorrichtung kann der Kartenbenutzer einen wählbaren Geldbetrag in die Börsenanwendung laden. Dem Börsenanbieter wird ein authentisches Zertifikat über den in die Börse geladenen und dem Konto des Börsenanbieters gutzuschreibenden Betrag zur Verfügung gestellt, ohne daß die zur Erstellung dieses Zertifikats notwendigen geheimen Daten in der Börsenanwendung bzw. im Börsenterminal gespeichert sein müssen.

DE 43 33 388 A1

Beschreibung

Die Erfindung betrifft ein System gemäß dem Oberbegriff des Hauptanspruchs.

Allgemein bekannt sind Karten, wie z. B. ec-Karten, Kreditkarten oder Telefonkarten mit integriertem Schaltkreis, die dem Benutzer für unterschiedliche Transaktionen zur Verfügung stehen. Die ec-Karten bzw. die Kreditkarten werden in zunehmendem Maß auch dazu verwendet, bargeldlose Transaktionen vom benutzereigenen Bankkonto auf ein beliebiges anderes Bankkonto zu veranlassen. Es handelt sich dabei im allgemeinen um Dienstleistungsanbieter oder Händler, die über ein entsprechendes Terminal verfügen, das der Kartenbenutzer zur Durchführung der Transaktionen benutzt.

Eine weitere Art der bargeldlosen Bezahlung bietet die sogenannte elektronische Börse. Um die Börse zu aktivieren, leistet der Kartenbenutzer eine Vorabzahlung an den Börsenanbieter und erhält dafür eine entsprechende Anzahl von Werteinheiten, die in der elektronischen Börse gespeichert werden. Bei jeder Inanspruchnahme einer Leistung wird die Börse um einen entsprechenden Betrag vermindert.

Aufgrund der zunehmenden Leistungsfähigkeit der in Karten eingesetzten integrierten Schaltkreise verstärken sich die Bestrebungen, sogenannte Multifunktionskarten vorzuschlagen, die es dem Benutzer erlauben, mit einer einzigen Karte die genannten Transaktionsarten (Bankanwendung, Börsenanwendung) zu nutzen.

Eine solche Multifunktionskarte hat im allgemeinen eine der kontoführenden Bank des Benutzers zugeordnete Bankanwendung und wenigstens eine einem Dienstanbieter oder Händler zugeordnete Börsenanwendung.

Aus der EP-OS 058 029 ist eine Multifunktionskarte mit Börsenfunktion bekannt. Die hier verwendete Multifunktionskarte unterscheidet mehrere Bankbereiche, einen Kreditkartenbereich und einen Börsenbereich. Dem Benutzer ist es mit Hilfe einer persönlichen Identifikationsnummer (PIN) möglich, zu einem Bank- bzw. Kreditkartenbereich Zugang zu erhalten. Der Benutzer kann nun aus diesem Bereich einen bestimmten Geldbetrag in den Börsenbereich umladen und diesen Betrag dann ohne PIN-Eingabe zur Inanspruchnahme von Dienstleistungen oder Waren nutzen.

Die EP-OS 058 029 enthält keinerlei Angaben darüber, wie der Ladevorgang gegen betrügerische Manipulationen gesichert ist.

Der Ladevorgang einer Börse wird im allgemeinen über eine im Verantwortungsbereich des Börsenanbieters liegende Vorrichtung (Terminal) abgewickelt. Dabei ist die im Verantwortungsbereich der Bank liegende Bankanwendung der Karte zwangsläufig in den Ladeprozeß einbezogen. Eine Kommunikation zwischen den in unterschiedlichen Verantwortungsbereichen liegenden Komponenten des Systems ist somit erforderlich, so daß es im Interesse aller am System beteiligten Institutionen notwendig ist, den gesamten Vorgang fälschungssicher zu gestalten und zu gewährleisten, daß die Integrität der in den einzelnen Komponenten des Systems notwendigen Geheiminformationen gewahrt bleibt.

Die Aufgabe der Erfindung besteht deshalb darin, ein System vorzuschlagen, das den obengenannten Problemen gerecht wird.

Die Aufgabe der Erfindung wird durch die im kennzeichnenden Teil des Hauptanspruchs angegebenen Merkmale gelöst.

Das Wesentliche der Erfindung besteht darin, dem Börsenanbieter ein authentisches Zertifikat über den in die Börse zu ladenden und dem Konto des Börsenanbieters gutzuschreibenden Betrag zur Verfügung zu stellen, ohne daß die zur Erstellung dieses Zertifikats notwendigen geheimen Daten in der Börsenanwendung bzw. im Börsenterminal gespeichert sein müssen.

Dazu wird in einem ersten Schritt des Umbuchungsvorgangs in der Bankanwendung über den vom Kunden gewählten Betrag und weiterer Transaktionsdaten mit nur in der Bankanwendung gespeicherten geheimen Daten ein Zertifikat erstellt, das dann innerhalb des integrierten Schaltkreises an die Börsenanwendung übertragen wird. In der Börsenanwendung wird zu diesem Transaktionszertifikat ein Authentisierungscode errechnet mit geheimen Daten, die ausschließlich in der Börsenanwendung bzw. im Terminal gespeichert sind. Transaktionszertifikat und Authentisierungscode werden zum Terminal übertragen und in diesem verifiziert. Ist der Vergleich positiv, so kann seitens des Börsenterminals davon ausgegangen werden, daß die gesendeten Daten authentisch sind.

In einem zweiten Schritt wird der Empfang echter Daten vom Börsenterminal dadurch bestätigt, daß dieses einen weiteren Authentisierungscode über die empfangenen Daten erstellt und an die Börsenanwendung zurücksendet. In der Börsenanwendung wird dieser zweite Authentisierungscode verifiziert. Ist der Vergleich positiv, kann seitens der Börsenanwendung davon ausgegangen werden, daß das Terminal ein echtes Transaktionszertifikat erhalten hat. Erst nach diesem Vergleich wird der vom Benutzer vorgewählte Betrag endgültig in den Börsenspeicher der Börsenanwendung übertragen. Die Umbuchung ist damit abgeschlossen.

Der Vorteil der Erfindung besteht darin, daß die Integrität der Geheimdaten der am System beteiligten Institutionen gewahrt bleibt. Bei der Implementierung mehrerer Börsenanwendungen in eine Multifunktionskarte sind keine gemeinsamen Schlüssel notwendig, um Beträge von der Bankanwendung in eine Börsenanwendung umzubuchen. Die einzelnen Börsen sind völlig unabhängig voneinander und arbeiten stets mit ihren eigenen Schlüsseln. Das Verfahren stellt sicher, daß das Börsenterminal ein Transaktionszertifikat erhält und dieses auch gültig ist. Erst nach einer entsprechenden Überprüfung wird der vom Benutzer gewählte Betrag in die Börse geladen. Mit dem Verfahren wird gleichzeitig sichergestellt, daß sowohl Terminal als auch Karte authentisch sind.

Vorzugsweise wird in der Bankanwendung vor der Erstellung des Transaktionszertifikats geprüft, ob der vom Kartenbenutzer gewählte Betrag kleiner ist als der in einem sogenannten Verfügungsrahmen gespeicherte Betrag. Der jeweils aktuelle Wert des Verfügungsrahmens stellt die Obergrenze des nutzbaren Geldbetrages dar. Ist der Verfügungsrahmen verbraucht, sind keine weiteren Umbuchungen in eine Börse möglich. Der Verfügungsrahmen kann nur durch eine durch vorherige PIN-Eingabe mögliche Transaktion mit der kontoführenden Bank des Kartenbenutzers wieder geladen werden. Diese Maßnahmen bewahren den Kartenbenutzer bei Verlust der Karte davor, daß zu große Beträge mißbräuchlich in die Börse umgebucht werden, solange die Börsenfunktion ohne vorherige PIN-Prüfung aktivierbar ist.

Gemäß einer Weiterbildung der Erfindung wird vorgeschlagen, in der Bankanwendung einen globalen

Transaktionszähler vorzusehen, der alle über die Bankanwendung laufenden Transaktionen zählt. Ein entsprechender Zähler ist für die Börsenanwendung vorgesehen. Nach jedem Umbuchungsvorgang von der Bankanwendung in die Börsenanwendung wird der Zählerstand des Transaktionszählers in der Bankanwendung in den Zählerstand des Transaktionszählers in der Börsenanwendung übertragen. Eine Umbuchung ist nur möglich, wenn der Zählerstand des Transaktionszählers in der Bankanwendung größer ist als der in der Börsenanwendung. Diese Maßnahme hat den Vorteil, daß bei einer gestohlenen Karte nur maximal eine Umbuchung vorgenommen werden kann, da ein zweiter Versuch wegen der Gleichheit der dann vorliegenden Zählerstände abgebrochen wird. Nur durch eine Transaktion mit der kontoführenden Bank, die eine PIN-Eingabe voraussetzt, wird der Transaktionszähler in der Bankanwendung erhöht, womit eine weitere Umbuchung freigegeben wird. Bei einer Karte mit mehreren Börsenanwendungen ist ein allen Börsen gemeinsamer Zähler vorgesehen.

Weitere Vorteile sowie Weiterbildungen der Erfindung sind Gegenstand der Unteransprüche sowie der nachfolgenden Beschreibung einer Ausführungsform der Erfindung, die anhand der Zeichnung beispielsweise beschrieben wird. Darin zeigen:

Fig. 1 eine schematische Darstellung des Informationsflusses zwischen den einzelnen Komponenten,

Fig. 2 ein Ablaufdiagramm des Umbuchvorgangs,

Fig. 3 ein Ablaufdiagramm des Bestätigungsvorganges.

Die Fig. 1 zeigt in einer beispielhaften Ausführungsform die wesentlichen Komponenten des erfindungsgemäßen Systems. Es besteht aus einer Multifunktionskarte 1 (MF) und einem Terminal 5 mit einer Schnittstelle 6 zur Kommunikation mit anderen Einheiten sowie einer Tastatur 7. Die Multifunktionskarte ist in drei Bereiche, den Bankbereich 2, den Börsenbereich 3 und den Systembereich 4 aufgeteilt. Auf den Bank- bzw. Börsenbereich können jeweils nur die dazu authorisierten Anbieter zugreifen. Der Systembereich enthält unter anderem allgemeine Daten, die von mehreren Anwendern genutzt werden können. Im folgenden soll nur auf die in den einzelnen Bereichen gespeicherten Daten und Vorgänge bzw. Programme eingegangen werden, die zum Verständnis der Erfindung notwendig sind.

Der in der Bankanwendung 2 gespeicherte Schlüssel S_{Bank} dient zusammen mit einem geeigneten Algorithmus zur Berechnung des bankspezifischen Zertifikats. Der Schlüssel ist nur der Bank bekannt bzw. nur in der Bankanwendung gespeichert. Ferner ist in der Bankanwendung ein sogenannter Verfügungsrahmen VR gespeichert, der den maximal vom Benutzer verfügbaren Betrag festlegt. Der Verfügungsrahmen ist also einem Betragslimit gleichzusetzen, über das der Benutzer ohne einen Authorisierungsvorgang mit der kontoführenden Bank verfügen kann. Ein aufgebrauchter Verfügungsrahmen kann nur durch einen PIN-gekoppelten und durch die kontoführende Bank authorisierten Prozeß initialisiert werden. Die in der Anwendung noch gespeicherte Kontonummer PAN und die Bankleitzahl BLZ dienen zur Identifikation des Benutzers gegenüber der Bank. Auf den in der Bankanwendung noch vorgesehenen Transaktionszähler GTZ wird später noch eingegangen.

Im Börsenbereich der Karte sind in der hier geschilderten beispielhaften Ausführungsform zwei Schlüssel $S_{Börse}$ und $S_{Börse}$ gespeichert, die der Authentisierung der Vorgänge zwischen der Börsenanwendung und dem Terminal dienen. Diese Schlüssel werden vom Börsenanwender ausgewählt bzw. von sogenannten Grundschlüsseln abgeleitet und sind nur dem Börsenanwender bekannt. Ferner enthält die Börsenanwendung wenigstens zwei Speicher BSRAM und BSS. Der RAM-Speicher dient zur vorübergehenden Speicherung des vom Benutzer für eine Umbuchung vorgesehenen Betrags. Erst nach Abschluß aller Authentisierungsvorgänge wird dieser Betrag in den Börsenspeicher transferiert. Schließlich enthält die Börsenanwendung einen Generator zur Erzeugung von Zufallszahlen RND.

Entsprechend der Börsenanwendung sind auch im Terminal die Börsenschlüssel $S_{Börse}$ und $S_{Börse}$ gespeichert. Zur Identifikation des Börsenterminals ist eine Terminal-Identifikationsnummer TID vorgesehen. Eine Terminal-Transaktionsnummer TTA wird bei jeder Buchung inkrementiert, so daß damit jeder Buchungsvorgang individualisiert wird. Der vom Benutzer über die Tastatur 7 eingegebene Geld- bzw. Transaktionsbetrag TB wird im Terminal zur weiteren Verarbeitung zwischengespeichert.

Der eigentliche Umbuchungsvorgang setzt sich aus zwei Kommandos, dem Kommando "Umbuchen" und dem Kommando "Bestätigen" zusammen. Der Ablauf dieser Kommandos ist in der Fig. 1 anhand von Signalverläufen grob skizziert und soll im folgenden anhand der Fig. 2 und 3 ausführlicher beschrieben werden.

Die Fig. 2 zeigt ein Ablaufdiagramm des Kommandos "Umbuchen". Das Terminal stellt zunächst einen Datensatz DAT_{Term} aus der von der Börsenanwendung der Karte angeforderten Zufallszahl RND, der Terminal-Identifikationsnummer TID, der Terminal-Transaktionsnummer TDA und dem Transaktionsbetrag TB zusammen. Durch die Verarbeitung einer Zufallszahl wird der Datensatz nicht vorhersehbar dynamisiert, was, wie an sich bekannt, gegen sogenannte replay-Angriffe schützt. Der Datensatz DAT_{Term} wird nun mit Hilfe des Börsenschlüssels $S1_{Börse}$ zur Erzeugung eines Echtheitscodes MAC_{Term} verschlüsselt. Der Datensatz DAT_{Term} und der Echtheitscode MAC_{Term} werden daraufhin in einem ersten Schritt des Umbuchungsvorgangs (siehe auch Fig. 1) an die Börsenanwendung übertragen. Diese berechnet jetzt ihrerseits aus dem Datensatz mit Hilfe des Börsenschlüssels $S1_{Börse}$ den Sicherheitscode MAC'_{Term}. Danach vergleicht die Börsenanwendung den errechneten Echtheitscode mit dem vom Terminal übermittelten Echtheitscode. Fällt dieser Vergleich negativ aus, wird hier, wie auch bei allen späteren Vergleichen, der Umbuchungsvorgang abgebrochen. Bei positivem Vergleich wird der Datensatz DAT_{Term} an die Bankanwendung übertragen. Hierbei handelt es sich zwar um einen anwendungsübergreifenden Prozeß, der jedoch ohne eine Absicherung durchgeführt werden kann, da er innerhalb des integrierten Schaltkreises durchgeführt wird. Für einen Fälscher bestehen auf dieser Ebene praktisch keine Zugriffsmöglichkeiten.

In der Bankanwendung wird nun zunächst geprüft, ob der Transaktionsbetrag TB kleiner ist als der durch den Verfügungsrahmen VR definierte Betrag. Bei positivem Vergleich wird der Transaktionsbetrag TB vom Verfügungsrahmen VR abgezogen. Daraufhin wird in der Bankanwendung überprüft, ob der Stand des globalen Transaktionszählers GTZ größer ist als der eines Börsentransaktionszählers BTZ, der, wie aus der Fig. 1 ersichtlich, im Systembereich der Multifunktionskarte gespeichert ist (BTZ). Wie schon erwähnt, wird nach jedem Umbuchungsvorgang von der Bankanwendung in die

Börsenanwendung der Zählerstand des globalen Transaktionszählers GTZ in den Transaktionszähler der Börsenanwendung BTZ übertragen. Eine Umbuchung ist nur möglich, wenn der Zählerstand des Zählers GTZ größer ist als der des Zählers BTZ. Diese Maßnahme bewirkt, daß bei einer gestohlenen Karte nur maximal eine Umbuchung vorgenommen werden kann. Nur durch eine Transaktion mit der kontoführenden Bank, die eine PIN-Eingabe voraussetzt, wird der Transaktionszähler GTZ in der Bankanwendung erhöht, womit eine weitere Umbuchung freigegeben wird. Sollen mehr als eine Umbuchung nach einer Transaktion mit der kontoführenden Bank möglich sein, sind entsprechende Zählerstände der genannten Zähler GTZ und BTZ bei einem Vergleich zu berücksichtigen.

Ergibt der Vergleich zwischen dem Transaktionszähler GTZ und dem Börsentransaktionszähler BTZ, daß eine Umbuchung möglich ist, wird der globale Transaktionszähler GTZ inkrementiert und der aktuelle Zählerstand des globalen Transaktionszählers GTZ in den Börsentransaktionszähler BTZ übertragen. Daraufhin wird in der Bankanwendung dem Datensatz DAT_{Term} die Kontonummer PAN und die Bankleitzahl BLZ hinzugefügt. Mit Hilfe des Schlüssels S_{Bank} wird aus dem Datensatz DAT_{Bank} der Echtheitscode MAC_{Bank} berechnet. Aus dem Datensatz DAT_{Bank} und dem Echtheitscode MAC_{Bank} wird das Zertifikat ZF_{Bank} erstellt. Dieses Zertifikat wird im dritten Schritt des Umbuchungsvorgangs an die Börsenanwendung übertragen.

In der Börsenanwendung wird nun zunächst der Transaktionsbetrag TB in den RAM-Speicher BSRAM übertragen. Daraufhin werden mit Hilfe der Schlüssel $S1_{Börse}$ und $S2_{Börse}$ die Echtheitscodes $MAC1_{Börse}$ und $MAC2_{Börse}$ aus dem Zertifikat ZF_{Bank} berechnet. Schließlich wird im vierten Schritt des Umbuchungsvorgangs das Zertifikat ZF_{Bank} mit dem Echtheitscode $MAC1_{Börse}$ an das Terminal übertragen.

Das Terminal berechnet jetzt seinerseits mit Hilfe des Schlüssels $S1_{Börse}$ den Sicherheitscode $MAC1'_{Börse}$ aus dem Zertifikat ZF_{Bank} und vergleicht die Echtheitscodes $MAC1_{Börse}$ und $MAC1'_{Börse}$. Ein positiver Vergleich bedeutet, daß das Zertifikat von einer authorisierten Börsenanwendung an das Terminal übertragen worden ist. Damit ist der Vorgang des Kommandos "Umbuchen" abgeschlossen.

Das Kommando "Bestätigen" wird, wie aus Fig. 3 ersichtlich, dadurch eingeleitet, daß im Terminal mit Hilfe des Schlüssels $S2_{Börse}$ der Echtheitscode $MAC2'_{Börse}$ aus dem Zertifikat ZF_{Bank} berechnet und an die Börsenanwendung übertragen wird.

In der Börsenanwendung wird der hier gespeicherte Echtheitscode $MAC2_{Börse}$ mit dem gesendeten Echtheitscode $MAC2'_{Börse}$ verglichen. Bei positivem Vergleich wird der Inhalt des RAM-Speichers in den Börsenspeicher BSS übertragen. Aufgrund des positiven Vergleichs ist seitens der Börsenanwendung sichergestellt, daß das Terminal ein authentisches Bankzertifikat erhalten und verarbeitet hat. In einem letzten Schritt wird der RAM-Speicher gelöscht und ein entsprechendes Signal über den erfolgreich durchgeführten Umbuchungsvorgang an das Terminal zurückgesendet.

Das Bankzertifikat ZF_{Bank} kann beispielsweise über die Schnittstelle 6 an die entsprechende Bank übertragen werden. Es ist auch möglich, mehrere Zertifikate im Terminal zu speichern und in bestimmten Abständen an die entsprechende Bank zu übertragen. Die Maßnahmen zur Absicherung derartiger Übertragungen sind bekannt, so daß darauf an dieser Stelle nicht näher eingegangen werden muß. Die Bank ist in der Lage, anhand des Bankschlüssels S_{Bank} das Zertifikat ZF_{Bank} auf Authentizität zu prüfen, um dann bei entsprechend positivem Vergleich anhand der im Zertifikat ZF_{Bank} übertragenen Daten den entsprechenden Betrag vom Konto des Kartenbenutzers auf das Konto des Börsenanbieters zu überweisen.

Patentansprüche

1. System zur Durchführung von Transaktionen mit einer Multifunktionskarte mit integriertem Schaltkreis, der eine der kontoführenden Bank des Benutzers zugeordnete Bankanwendung und wenigstens eine einem Dienstleistungsanbieter oder Händler zugeordnete Börsenanwendung enthält und mit einer Vorrichtung, über die ein wählbarer Geldbetrag in die Börsenanwendung geladen werden kann, indem unter anderem den Geldbetrag enthaltende Transaktionsdaten von der Vorrichtung an die Karte übertragen und innerhalb des integrierten Schaltkreises der Karte von der Bankanwendung in die Börsenanwendung umgeladen wird, **dadurch gekennzeichnet**, daß
   - von den von der Vorrichtung übertragenen Transaktionsdaten innerhalb der Bankanwendung ein Transaktionszertifikat unter Verwendung geheimer, nur der Bank bzw. in der Bankanwendung gespeicherter Daten erstellt wird,
   - das Transaktionszertifikat in die Börsenanwendung übertragen wird und
   - der umzubuchende Geldbetrag erst dann in die Börsenanwendung geladen wird, wenn die Vorrichtung den Empfang des durch die Börsenanwendung authentisierten Transaktionszertifikats gegenüber die Börsenanwendung bestätigt.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß das von der Börsenanwendung zur Vorrichtung übertragene Transaktionszertifikat sowie die Bestätigung der Vorrichtung über den Erhalt des Transaktionszertifikats durch geheime Daten authentisiert wird, die nur dem Dienstleistungsanbieter oder Händler bekannt und in der Börsenanwendung sowie in der Vorrichtung gespeichert sind.

3. System nach Anspruch 2, dadurch gekennzeichnet, daß zur Authentisierung des Transaktionszertifikats in der Börsenanwendung mit Hilfe eines ersten Börsenschlüssels ein Authentisierungscode berechnet wird, daß das Transaktionszertifikat und der Authentisierungscode zur Vorrichtung übertragen werden und daß in der Vorrichtung der Authentisierungscode mit Hilfe des ersten Börsenschlüssels verifiziert wird.

4. System nach Anspruch 3, dadurch gekennzeichnet, daß in der Vorrichtung mit Hilfe eines zweiten Börsenschlüssels aus dem Transaktionszertifikat eine zweiter Authentisierungscode berechnet wird, daß dieser Authentisierungscode zur Börsenanwendung übertragen wird und daß der zweite Authentisierungscode in der Börsenanwendung verifiziert wird.

5. System nach Anspruch 1, dadurch gekennzeichnet, daß vor der Übertragung der Transaktionsdaten von der Vorrichtung an die Börsenanwendung in der Vorrichtung ein Authentisierungscode gebildet wird, der gemeinsam mit den Transaktionsda-

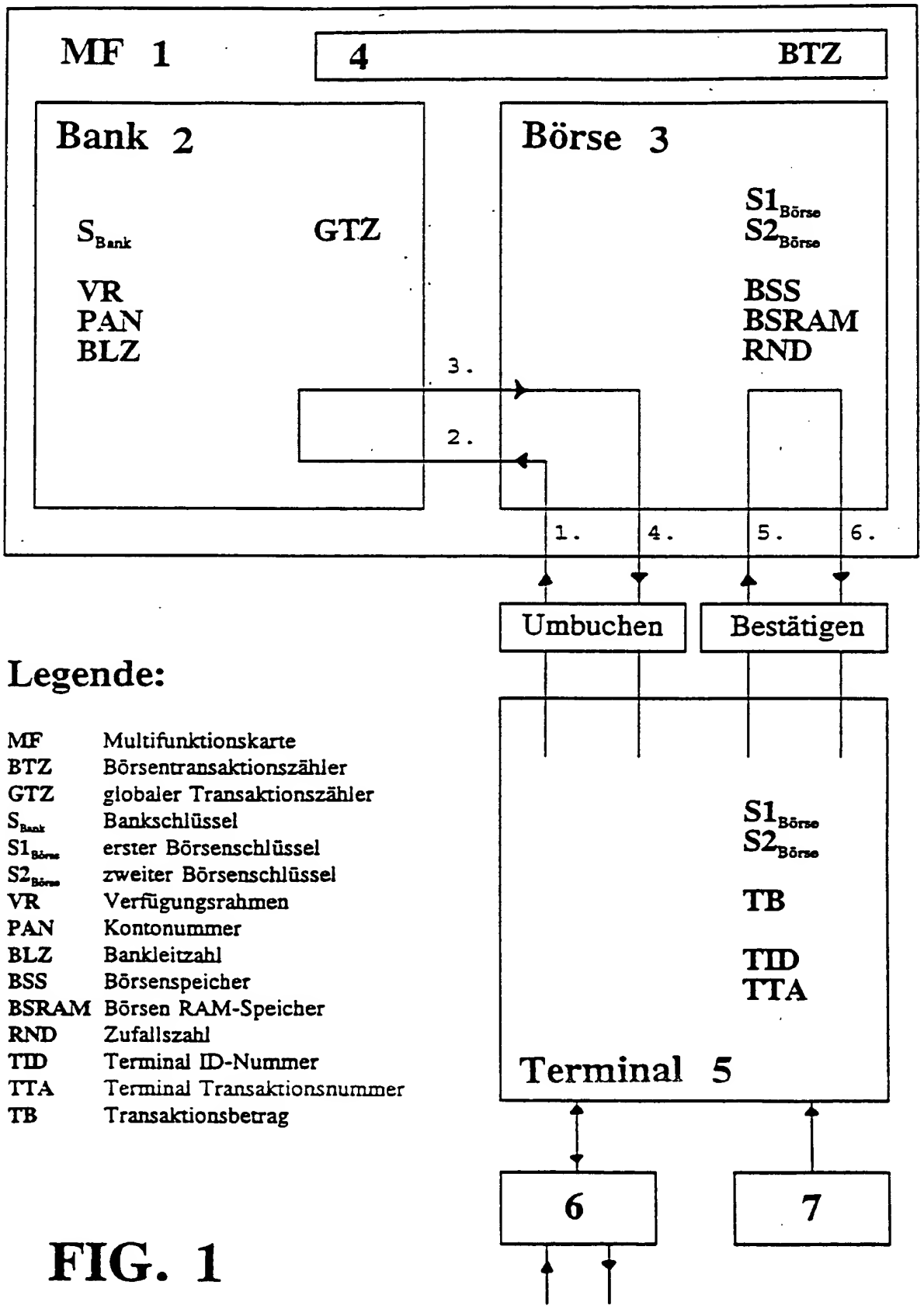
ten an die Börsenanwendung übertragen und in dieser verifiziert wird.

6. System nach Anspruch 1, dadurch gekennzeichnet, daß vor der Bildung des Transaktionszertifikats in der Bankanwendung geprüft wird, ob der umzubuchende Geldbetrag innerhalb eines in der Bankanwendung definierten Verfügungsrahmens liegt.

7. System nach Anspruch 1 oder 6, dadurch gekennzeichnet, daß vor der Bildung des Transaktionszertifikats in der Bankanwendung festgestellt wird, ob die Anzahl der mit der Karte durchgeführten Umbuchungen einen einstellbaren Wert überschreitet.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 43 33 388 A1
Int. Cl.[6]: G 07 F 19/00
Offenlegungstag: 6. April 1995



Legende:

MF	Multifunktionskarte
BTZ	Börsentransaktionszähler
GTZ	globaler Transaktionszähler
S_{Bank}	Bankschlüssel
$S1_{Börse}$	erster Börsenschlüssel
$S2_{Börse}$	zweiter Börsenschlüssel
VR	Verfügungsrahmen
PAN	Kontonummer
BLZ	Bankleitzahl
BSS	Börsenspeicher
BSRAM	Börsen RAM-Speicher
RND	Zufallszahl
TID	Terminal ID-Nummer
TTA	Terminal Transaktionsnummer
TB	Transaktionsbetrag

FIG. 1

Nummer: DE 43 33 388 A1
Int. Cl.[6]: G 07 F 19/00
Offenlegungstag: 6. April 1995

Umbuchen

Terminal: $DAT_{Term} = (RND, TID, TTA, TB)$
$S1_{Börse}(DAT_{Term}) => MAC_{Term}$

1. DAT_{Term}, MAC_{Term} --> Börse

Börse: $S1_{Börse}(DAT_{Term}) => MAC'_{Term}$
$MAC_{Term} = MAC'_{Term}$

2. DAT_{Term} --> Bank

Bank: $TB <= VR$
$VR = VR - TB$
$GTZ > BTZ$
$GTZ = GTZ + 1$
$DAT_{Bank} = (DAT_{Term}, PAN, BLZ)$
$S_{Bank}(DAT_{Bank}) => MAC_{Bank}$
$ZF_{Bank} = (DAT_{Bank}, MAC_{Bank})$
GTZ --> BTZ

3. ZF_{Bank} --> Börse

Börse: TB --> $BSRAM$
$S1_{Börse}(ZF_{Bank}) => MAC1_{Börse}$
$S2_{Börse}(ZF_{Bank}) => MAC2_{Börse}$

4. $ZF_{Bank}, MAC1_{Börse}$ --> Terminal

Terminal: $S1_{Börse}(ZF_{Bank}) => MAC1'_{Börse}$
$MAC1_{Börse} = MAC1'_{Börse}$

FIG. 2

Nummer: DE 43 33 388 A1
Int. Cl.[6]: G 07 F 19/00
Offenlegungstag: 6. April 1995

Bestätigen

Terminal: $S2_{Börse}(ZF_{Bank}) => MAC2'_{Börse}$

5. MAC2'$_{Börse}$ --> Börse

Börse: $MAC2_{Börse} = MAC2'_{Börse}$
BSRAM --> BSS
BSRAM löschen

6. o.k. --> Terminal

FIG. 3

Method for cash sum transfer into and from smart cards

Patent number: DE4243851
Publication date: 1994-06-30
Inventor: ENDLER REINHARD [DE]; WESTPHAL REINHARD [DE]; HARTLEIF SIEGFRIED [DE]; NIEHAUS HERBERT [DE]; SCHAEFER PETER [DE]; MERGEMEIER DETLEV [DE]; HOVEMEYER DIETER [DE]
Applicant: DEUTSCHE BUNDESPOST TELEKOM [DE];; IBM [US];; ORGA DATENTECH GMBH [DE];; GAD GES FUER AUTOMATISCHE DATE [DE]
Classification:
- International: G06F15/21; G07F7/08; G06K19/07; B42D15/10
- european: G07F7/08C; G07F7/08C2C
Application number: DE19924243851 19921223
Priority number(s): DE19924243851 19921223

Also published as:
EP0605070 (A2)
EP0605070 (A3)
EP0605070 (B1)

Abstract not available for DE4243851
Abstract of corresponding document: **EP0605070**

2.1 Known methods are based on the idea that debiting and crediting exchange functions operate independently of each other. The solution according to the invention is based on the object of combining the advantages of crediting exchange with the advantages of debiting exchange. 2.2 According to the invention, overwritable memory areas of a smart card are divided up into a memory area for crediting exchange functions and at least one memory area for debiting exchange functions. Using the application program of the smart card, together with the program of an authorization system, a cash sum from the crediting exchange is transferred, once or repeatedly in succession, into the debiting exchange. 2.3 By the solution according to the invention, the user of the service is able by means of just one multifunctional smart card to fill the debiting exchange of the smart card at any time from the credit afforded him in the crediting exchange.